**ASSIGNMENT-4**

A black and gold logo

Description automatically generated

**Virtualization and Cloud Computing, Conestoga College**

**SYST8171: Adoption and Migration Planning for Virtualization**

**Submitted By: Swathi Anil (8905477)**

**Submitted To: Prof Vignesh Ravi**

**16-07-2024**

# Rainyday Grocer Cloud Migration Risk Assessment

# Executive Summary

The online grocery delivery business of Rainyday Grocer (RG) is converting to a Microservices Architecture (MSA) hence it is put in the cloud. The following document aims at conducting a risk analysis of cloud adoption and migration of RG company and suggestions on measures to avoid the risks.

## Key Findings

* Data Breach during Migration: High probability and high risk.
* Misconfiguration of Cloud Services: Moderate likelihood and high potential effect.
* Security Vulnerabilities in Microservices: Most likely and high consequence.

## Recommendations There is a need to enhance  encryption and other secure methods of data transfer during migration. Finally, Continuous Monitoring and Automated Configuration Management need to be used. Implement DevSecOps practice at the center of the software development life cycle.

# Introduction

Rainyday Grocer is moving from Monolith in the cloud to Microservices Architecture (MSA) which is also deployed in the cloud. RG is a customized online grocery delivery business. RG focuses on customers who need groceries on rainy days as they are unable to go to the store on rainy days. RG provides its customers with multiple ordering options as well as delivery options. Another attraction of RG is that they don’t own inventory, distribution channels, supply channels, or any data centers. They rely on other service providers for all types of services. In this particular assignment several checks on the basis of cloud adoption and migration will be conducted, we will also establish the possible threats and proposals for the migration plan.

# Risk Assessment Approach

Quantitative method is used by the Risk assessment in evaluating the risks. This risk assessment is based on an impact and its likelihood. After that, we will outline 10 possible threats that can be connected with cloud adoption and migration. Three threats will be chosen that can be most unsafe for further analysis and indicating the measures that should be taken, in order to manage these risks.

# Risk Identification and Assessment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Event Activity | Potential Risk | Likelihood (L) | Impact (I) | Risk Level (L \* I) | Risk Rating | Controls |
| Data Migration | Data Breach | 4 | 5 | 4\*5=20 | Extreme | * The use of HTTPS and SFTP shall be employed for file transfer. * VPN is used in data transmission. * Managing the data access. |
| Microservices Development | Security Vulnerabilities | 3 | 5 | 3\*5=15 | High | * Support the DevSecOps culture to maintain security. * The company should conduct frequent Vulnerability tests. * It is recommended to perform penetration testing once in a while. |
| Cloud Configuration | Misconfiguration | 3 | 5 | 3\*5=15 | High | * Using automated configuration management eg: Terraform which helps users to write infrastructure code. * Using AWS config for monitoring. * Inspect for security purposes, for the latest audits. |
| Service Migration | Service Downtime | 3 | 4 | 3\*4=12 | High | * Consider the use of backup plans together with systems. * Monitoring tools should be activated to function as planned.. * Backup data especially in a form that cannot be easily stolen or destroyed. |
| IAM Policy Management | Insufficient IAM Policies | 3 | 4 | 3\*4=12 | High | * Ensure to adhere to IAM policies. * Revise IAM guidelines. * Immersive practical training is required to be provided to all the staff members and regular updates must be conveyed on IAM. |
| Technical | Isolation Failure | 3 | 4 | 3\*4=12 | High | * The setting requires a Strong Isolation Mechanism. * Regularly test audits. |
| Policy & Organizational | Loss of Governance | 3 | 4 | 3\*4=12 | High | * Set up a governance structure. * Regular Reviews. * Make amendments to policies as the case may be |
| Technical | Loss of Encryption Keys | 3 | 5 | 3\*5=15 | High | * Key Management Systems. * Regular Key Rotation. * Access Controls |
| Backup and Recovery | Inadequate Processes | 3 | 4 | 3\*4=12 | High | * Regular Backups. * Recovery Plan * Testing |
| Cloud Service Use | Vendor Lock-in | 2 | 3 | 2\*3=6 | Moderate | * Multi-cloud Strategy. * Open Standards |
| Compliance Management | Regulatory Failures | 3 | 4 | 3\*4=12 | High | * Compliance Checks. * Training. * Audits |
| Data Transmission | Data Loss | 2 | 4 | 2\*4=8 | Moderate | * Redundancy * Monitoring. * Protocols |
| Service Operation | Service Operation | 3 | 3 | 3\*3=9 | Moderate | * Monitoring, Optimization, Scaling |
| Policy & Organizational | Cloud Provider Acquisition | 2 | 4 | 2\*4=8 | Moderate | * Contract Clauses. * Multi-cloud Strategy |

# Risk Evaluation and Migration

## Risk Prioritization

1. Data Breach during Migration
2. Security Vulnerabilities in Microservices Development
3. Misconfiguration of cloud services

# Risk Treatment Strategy

## Data Breach during Migration

**Justification:** When migrating, it is possible to lose a lot of data, and this might cause a company’s financial loss as well as harm its reputation. As clients’ data contain rather sensitive information and their leakage may cost certain consequences, this risk is considered to be essential.

**Risk Treatment Strategy:** This should be done by having a good encryption process/data transfer method, and these should be accompanied by strict security measures.

**Controls:**

**Encryption**: The AES-256 encryption makes sure that data is slightly protected when transferring; supposing it is stored since it would be very hard for another person to access the information or even understand it if they gets it.

**Secure Transfer Protocols:** Deployment of HTTPS and SFTP minimizes the problem of interception and alteration of data as it will be transferred securely over the network.

**Virtual Private Network (VPN):** The network connection created by setting up a VPN for the transfer of data also provides an encrypted pathway for the information which also reduces its vulnerability to interception.

**Access Controls:** The least number of people that can get a hold of the data is also an effective measure to control internal threat as only the people who are authorized to deal with the data can do so.

## Challenges of Internal Security in the Development of Microservices

**Justification:** The security or lack of security in some microservices may cause a compromise of the resources, unauthorized access, leakage of data, and therefore compromise the entire service.

**Risk Treatment Strategy:** Implement the DevSecOps reassure and scan regularly for vulnerabilities. They also use pen-test to remain safe in the development processes.

**Controls:**

**Integration of DevSecOps:** DevSecOps entails the incorporation of security measures across the developmental and operational procedures to champion security as the norm from the onset of the development to the application’s distribution and usage.

**Regular Vulnerability Scans:** Scanning for vulnerabilities is a powerful tool that can be used to discover and eliminate the holes in the security system before attackers manage to get access to them.

**Penetration Testing:** Performing penetration testing periodically means replicating an attack at the system to discover that the routine security scans might overlook, so that to prevent such issues.

## Misconfiguration of Cloud Services

**Justification:** SDD vulnerabilities can lead to unauthorized accessibility, data leakages, and service disruption since misconfigurations give access to these areas. Due to the fact that cloud networks are elaborate and constantly evolving, this risk is rather high.

Risk Treatment Strategy: This can be done with the use of configuration automatically management, using monitoring services, and, periodical check up.

Controls:

Automated Configuration Management: Tasks such as configuration management are made easy through the help of Application orchestration tools such as Terraform, this helps to get rid of human errors made during configuration and changes.

Continuous Monitoring: Use of continuous monitoring which is provided by AWS Config technology is useful in real time detection of changes in the services and also compliance to best practices.

Regular Audits: This way, simple and thorough audits check configurations for any deviation to the security and compliance to relevant standards of the industry or by standards set to govern the specific field of practice.

# Shared Responsibility Model Consideration

## CSP Responsibility

* Security of physical data center.
* Security of Infrastructure such as hardware, software, network, & physical structures.

## Responsibility of Customers

* Data protection and encryption.
* Identity and Access Management is one of the company’s functional areas, and this functional area mainly deals with the issue of security.
* Application-level security.
* Client and endpoint protection.
* The configurations of using cloud services and its applicability.

# Conclusion

The risk analysis of RG’s cloud adoption and migration identifies focal points that need attention and measures to reduce the major risks. Thus, the application of effective controls and adherence to the shared responsibility model can increase the security and reliability of RG’s MSA-based cloud solution. The mentioned interventions contribute to enhancing the quality of data protection and service delivery, as well as meeting the requirement of the chosen industry.

# Reference

*How To Implement NIST 800-30 in Risk Assessments | HyperComply Blog*. (n.d.). Www.hypercomply.com. <https://www.hypercomply.com/blog/nist-800-30#:~:text=NIST%20800%2D30%20acts%20as>

*3 Cloud Migration Risks and How to Avoid Them Successfully*. (2022, August 24). Helixstorm. <https://www.helixstorm.com/blog/cloud-migration-risks-and-how-to-avoid-them-successfully/>

Chaudhary, A. (2023, August 14). *Managing Cloud Misconfigurations Risks | CSA*. Cloudsecurityalliance.org. <https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks>

*Data Migration Risks And The Checklist You Need To Avoid Them*. (2023, March 24). Monte Carlo Data. <https://www.montecarlodata.com/blog-data-migration-risks-checklist/>

*Evaluate and mitigate migration risks | Migration Center*. (n.d.). Google Cloud. <https://cloud.google.com/migration-center/docs/migration-risks>

Michan, D. (2023, July 29). *Comprehensive Guide to Mitigating Data Migration Risks*. Www.cybersecurityhq.io. <https://www.cybersecurityhq.io/blog/comprehensive-guide-to-mitigating-data-migration-risks>

*Microservices security: 6 Best practice tips | Snyk*. (2022, February 10). Snyk.io. <https://snyk.io/learn/microservices-security/>

S, N. (2023, May 4). *Cloud Migration Strategy Blueprint: Benefits, Types, and Challenges*. Www.cloudpanel.io. <https://www.cloudpanel.io/blog/cloud-migration-strategy/>

*Security Archives*. (2024, July 16). OpenText Blogs. <https://blogs.opentext.com/category/technologies/security/>

Soldani, J., & Brogi, A. (2023). Microservices Security: Bad vs. Good Practices. *Lecture Notes in Computer Science*, 337–352. <https://doi.org/10.1007/978-3-031-36889-9_23>